Discrete Applied Mathematics 41 (1993) 223–233
North-Holland

Balance, uncorrelatedness and the strict avalanche criterion

Sheelagh Lloyd

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS12 6QZ, UK

Received 26 May 1989
Revised 18 October 1990

Abstract

Lloyd, S., Balance, uncorrelatedness and the strict avalanche criterion, Discrete Applied Mathematics 41 (1993) 223–233.

A number of criteria have been proposed in the literature for cryptographic transformations. We explore here the connections between three of these: balance, uncorrelatedness and the strict avalanche criterion. Our main result is that there are no balanced, uncorrelated functions which satisfy the strict avalanche criterion of order $n - 2$.

Introduction

In this paper we shall investigate the connections between three criteria which have each been proposed as desirable for cryptographic transformations. These three criteria are balance, uncorrelatedness and the higher order strict avalanche criterion. For a function to be balanced, all output vectors must be equally likely if all input vectors are equally likely. A function is uncorrelated if, given any input vector and its corresponding output vector, then the probability that any particular input bit is equal to any particular output bit is equal to $\frac{1}{2}$. For a function to fulfil the strict avalanche criterion, each output bit should change with probability $\frac{1}{2}$ whenever a single input bit is changed. The notion of higher order strict avalanche criterion was introduced by Forré [1] to consider subfunctions obtained from the original function by keeping one or more input bits constant.

Although all these criteria can be applied to functions from n bits to m bits, we

Correspondence to: Dr. S. Lloyd, Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS12 6QZ, UK.

shall concentrate simply on the case $m = 1$. Obviously, any function from n bits to m bits can be thought of as a collection of m functions each from n bits to one bit. If the original function is balanced, then each of the m functions must be balanced, although the converse is not true. The original function is uncorrelated if and only if each of the m functions is, and the same is true for functions satisfying the strict avalanche criterion. So certainly if the original function is to satisfy any combination of these three criteria, then each of the m functions must satisfy that combination too. Thus we are justified in considering only the case $m = 1$.

In the first section, we shall give formal definitions of all three criteria, and present some alternative formulations which will be of use later in the paper. In the second section, we shall consider when functions satisfying a higher order strict avalanche criterion can also be balanced. The third section is devoted to consideration of uncorrelatedness, and its connections with the other two criteria. The main result is that there are no balanced, uncorrelated functions satisfying the strict avalanche criterion of order $n-2$.

1. Definitions

In this section we shall define the three properties, and present an important characterisation of functions satisfying a higher order strict avalanche criterion. We shall find it useful to express these criteria in terms of the associated function $\hat{f}: \mathbb{Z}_2^n \to \{1, -1\}$ defined by $\hat{f}(\boldsymbol{x}) = (-1)^{f(\boldsymbol{x})}$, so we shall follow each definition with the corresponding condition on $\hat{f}$.

In what follows, all the summations will be computed over $\mathbb{Z}^n$. This is an abuse of notation, since sometimes the objects being summed are elements of $\mathbb{Z}_2^n$ but we hope that the intentions are clear.

Definition 1.1. Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a cryptographic transformation. Then f is said to be *balanced* if half the input vectors are mapped onto zero and half are mapped onto one.

Lemma 1.2. *Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a cryptographic transformation. Then f is balanced if and only if*

$$\sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} \hat{f}(\boldsymbol{x}) = 0.$$

Proof. Immediate. □

Definition 1.3. Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a cryptographic transformation. Then f is said to be *uncorrelated* if, given that $\boldsymbol{x}$ satisfies $f(\boldsymbol{x}) = 1$, the probability that any particular bit of $\boldsymbol{x}$ is equal to one is $\frac{1}{2}$. In other words, f is uncorrelated if and only if

$$\sum_{\substack{x \in \mathbb{Z}_2^n \\ f(x)=1}} x = \left(\frac{N}{2}, \ldots, \frac{N}{2}\right)$$

where N is the size of the inverse image of 1 under f (equivalently, the number of input vectors mapped onto 1 by f).

Lemma 1.4. *Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$, and let N be the size of the inverse image of 1 under f. Then f is uncorrelated if and only if*

$$\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) \cdot x = (2^{n-1} - N, \ldots, 2^{n-1} - N).$$

Proof. Let us write

$$S_0 = \sum_{\substack{x \in \mathbb{Z}_2^n \\ f(x)=0}} x \quad \text{and} \quad S_1 = \sum_{\substack{x \in \mathbb{Z}_2^n \\ f(x)=1}} x.$$

Then

$$S_0 - S_1 = \sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) \cdot x$$

and

$$\begin{aligned} S_0 + S_1 &= \sum_{x \in \mathbb{Z}_2^n} x \\ &= (2^{n-1}, \ldots, 2^{n-1}) \end{aligned}$$

so

$$\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) \cdot x = (2^{n-1}, \ldots, 2^{n-1}) - 2S_1.$$

Now f is uncorrelated if and only if S_1 is equal to $(N/2, \ldots, N/2)$, so we have the desired result. □

Definition 1.5 [3]. Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ be a cryptographic transformation. Then f satisfies the strict avalanche criterion (SAC) if and only if

$$\sum_{x \in \mathbb{Z}_2^n} f(x) \oplus f(x \oplus c_i) = (2^{n-1}, \ldots, 2^{n-1}), \quad \text{for all } i,\ 1 \le i \le n$$

where $\oplus$ denotes bitwise exclusive or and c_i is the vector of length n with a 1 in the ith position and 0 elsewhere.

Definition 1.6 [1]. A function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order m, where $1 \le m \le n-2$ if and only if any function obtained from f by keeping m of its input bits constant satisfies the SAC (for any choice of the positions and of the values of the constant bits).

Theorem 1.7 [2]. *Suppose that $n \in \mathbb{Z}$, $n \ge 2$ and $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$. Then f satisfies the SAC of order $n-2$ if and only if for all $S \subseteq \{1, 2, \ldots, n\}$,*

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{|S|(|S|-1)/2}(\hat{f}(\mathbf{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}})$$

where $\boldsymbol{e}_S$ *denotes the element of* $\mathbb{Z}_2^n$ *which satisfies* $e_i = 1 \Leftrightarrow i \in S$.

This theorem may also be stated in terms of f in a more natural way as follows.

Theorem 1.8. *Suppose that* $n \in \mathbb{Z}$, $n \geq 2$ *and* $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. *Then* f *satisfies the SAC of order* $n-2$ *if and only if*

$$f(\boldsymbol{x}) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} x_i x_j$$

for some $a_0, a_1, \ldots, a_n \in \mathbb{Z}_2$.

Proof. We look more closely at the condition derived in Theorem 1.7, and write it in terms of f rather than $\hat{f}$. The condition is that

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{|S|(|S|-1)/2}(\hat{f}(\mathbf{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}})$$

for all $S \subseteq \{1, 2, \ldots, n\}$. Now $|S|(|S|-1)/2$ is just the number of pairs of distinct elements $i, j \in S$, so we may rewrite this as

$$\hat{f}(\boldsymbol{e}_S) = \hat{f}(\mathbf{0}) \prod_{i \in S} (\hat{f}(\mathbf{0})\hat{f}(\boldsymbol{e}_{\{i\}})) \prod_{1 \leq i < j \leq n} (-1)$$

which is equivalent to

$$f(\boldsymbol{e}_S) = f(\mathbf{0}) \oplus \bigoplus_{i \in S} (f(\mathbf{0}) \oplus f(\boldsymbol{e}_{\{i\}})) \oplus \bigoplus_{i,j \in S, i<j} 1.$$

We recall that $\boldsymbol{e}_S$ satisfies $e_i = 1 \Leftrightarrow i \in S$, so the above becomes

$$f(\boldsymbol{x}) = f(\mathbf{0}) \oplus \bigoplus_{i=1}^{n} (f(\mathbf{0}) \oplus f(\boldsymbol{e}_{\{i\}}))x_i \oplus \bigoplus_{1 \leq i < j \leq n} x_i x_j.$$

So we see that f satisfies the SAC of order $n-2$ if and only if the above condition holds. Putting $a_0 = f(\mathbf{0})$, $a_i = f(\mathbf{0}) \oplus f(\boldsymbol{e}_{\{i\}})$ for $i = 1, \ldots, n$ yields the desired result. □

2. Balance

We want to consider functions $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ which satisfy the strict avalanche criterion of order $n-2$, and which are also balanced.

Lemma 2.1. *Suppose* $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ *satisfies the SAC of order* $n-2$. *Then*

$$\sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} \hat{f}(\boldsymbol{x}) = \Im[(1 + i\hat{f}(\mathbf{0})) \prod_{r=1}^{n} (1 + i\hat{f}(\boldsymbol{e}_{\{r\}}))]$$

where $\Im$ *denotes the imaginary part.*

Proof. Let us denote the left-hand side of the above equation by L, and the product on the right-hand side by P. Then we want to show that $L = \Im(P)$.

Since f satisfies the SAC of order $n-2$, we know that for all $S \subseteq \{1, 2, \ldots, n\}$,

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{|S|(|S|-1)/2}(\hat{f}(\mathbf{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}}).$$

Let us consider two cases separately. If $|S|$ is odd, then $\hat{f}(\mathbf{0})^{(|S|+1)} = 1$, and $(-1)^{|S|(|S|-1)/2} = (-1)^{(|S|-1)/2}$ and so

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{(|S|-1)/2} \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}}).$$

On the other hand, if $|S|$ is even, then

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{|S|/2}(\hat{f}(\mathbf{0})) \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}}).$$

So each term of the sum L is the product of an odd number m of the terms $\hat{f}(\mathbf{0})$, $\hat{f}(\boldsymbol{e}_{\{r\}})$ with the multiplier $(-1)^{(m-1)/2}$, and all possible such products appear in the sum. For example, in the case $n = 2$, the sum is

$$\hat{f}(00) + \hat{f}(01) + \hat{f}(10) - \hat{f}(00)\hat{f}(01)\hat{f}(10).$$

Consider now the product P. The terms in the expansion of P are products of a number m of the terms $\hat{f}(\mathbf{0})$, $\hat{f}(\boldsymbol{e}_{\{r\}})$ with the multiplier i^m. Now, if m is odd, then $i^m = (-1)^{(m-1)/2} i$, and if m is even, then $i^m = (-1)^{m/2}$. So we see that L is precisely the imaginary part of P as required. □

Corollary 2.2. *Suppose $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Suppose further that exactly m of the input vectors $\mathbf{0}$, $\boldsymbol{e}_{\{r\}}$ are mapped onto 1 by f. Then*

$$\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) = 2^{(n+1)/2} \sin \frac{\pi}{4}(n + 1 - 2m).$$

Proof. From Lemma 2.1, we see that

$$\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) = \Im[(1-i)^m (1+i)^{n+1-m}].$$

Now

$$(1+i)^N = 2^{N/2}\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right)^N = 2^{N/2}\left(\cos N\frac{\pi}{4} + i \sin N\frac{\pi}{4}\right)$$

so

$$\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) = 2^{(n+1)/2}\Im\left[\left(\cos m\frac{\pi}{4} - i \sin m\frac{\pi}{4}\right) \times \left(\cos(n+1-m)\frac{\pi}{4} + i \sin(n+1-m)\frac{\pi}{4}\right)\right]$$

$$= 2^{(n+1)/2}\left(\sin(n+1-m)\frac{\pi}{4}\cos m\frac{\pi}{4} - \sin m\frac{\pi}{4}\cos(n+1-m)\frac{\pi}{4}\right)$$

$$= 2^{(n+1)/2}\sin(n+1-2m)\frac{\pi}{4}. \quad \square$$

Lemma 2.3. *Suppose $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Suppose further that exactly m of the input vectors $\mathbf{0}, \boldsymbol{e}_{\{r\}}$ are mapped onto 1 by f. Then f is balanced if and only if $n+1-2m \equiv 0 \pmod 4$.*

Proof. By Corollary 2.2, f is balanced if and only if $\sin(\pi/4)(n+1-2m) = 0$ which happens exactly when $n+1-2m \equiv 0 \pmod 4$. Hence f is balanced exactly when $n+1-2m \equiv 0 \pmod 4$. $\square$

We are now able to prove our two main results on balance and the strict avalanche criterion.

Theorem 2.4. *Let n be an even integer. Then there are no balanced functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$.*

Proof. Suppose, for a contradiction, that $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$ and is balanced. By Lemma 2.3, the number m of the input vectors $\mathbf{0}, \boldsymbol{e}_{\{r\}}$ which are mapped by f onto 1 must satisfy the congruence $1+n-2m \equiv 0 \pmod 4$. But if n is even, then this congruence has no solution. So there are no such functions f. $\square$

Theorem 2.5. *Let n be an odd integer. Then exactly half of the functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$ are also balanced.*

Proof. By Lemma 2.3, the number m of the input vectors $\mathbf{0}, \boldsymbol{e}_{\{r\}}$ which are mapped by f onto 1 must satisfy the congruence $1+n-2m \equiv 0 \pmod 4$. Now any function satisfying the SAC of order $n-2$ is completely determined by its values at these $n+1$ vectors, so for each m there are exactly $\binom{n+1}{m}$ such functions.

If $n \equiv 3 \pmod 4$, then $m \equiv 0 \pmod 2$, so the number of functions is

$$M = \binom{n+1}{0} + \binom{n+1}{2} + \cdots + \binom{n+1}{n+1}$$

$$= 2^n.$$

If $n \equiv 1 \pmod 4$, then $m \equiv 1 \pmod 2$, so the number of functions is

$$M = \binom{n+1}{1} + \binom{n+1}{3} + \cdots + \binom{n+1}{n}$$

$$= 2^n.$$

The total number of functions satisfying the SAC of order $n-2$ is 2^{n+1}. In both cases, therefore, we see that exactly half of the functions satisfying the SAC of order $n-2$ are balanced. □

We have the interesting corollary.

Corollary 2.6. *Let n be an odd integer, and suppose that $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Then f is balanced if and only if*

$$f(\boldsymbol{x} \oplus (1, \ldots, 1)) = f(\boldsymbol{x}) \oplus 1, \quad \textit{for all } \boldsymbol{x} \in \mathbb{Z}_2^n.$$

Clearly, if f satisfies the above condition, then it is balanced, since each input vector may be matched with its complement. It is perhaps surprising that the converse is also true.

In order to prove this result, we need a lemma which will also be useful later on.

Lemma 2.7. *Let n be an odd integer, and suppose that $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Suppose further that exactly m of the input vectors $\mathbf{0}, \boldsymbol{e}_{\{r\}}$ are mapped by $\hat{f}$ to -1. Then*

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) \cdot \hat{f}(\boldsymbol{x}) = (-1)^{(n-1)/2}(-1)^m, \quad \textit{for all } \boldsymbol{x} \in \mathbb{Z}_2^n.$$

Proof. Since f satisfies the SAC of order $n-2$, we know that

$$\hat{f}(\boldsymbol{e}_S) = (-1)^{|S|(|S|-1)/2}(\hat{f}(\mathbf{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\boldsymbol{e}_{\{r\}})$$

for all subsets S of $\{1, \ldots, n\}$. Now if $\boldsymbol{x}$ corresponds to the subset S, then $\boldsymbol{x} \oplus (1, \ldots, 1)$ corresponds to $\{1, \ldots, n\} \setminus S$. Hence

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) \cdot \hat{f}(\boldsymbol{x}) = (-1)^{n(n-1)/2}(-1)^{|S|(n-|S|)}(\hat{f}(\mathbf{0}))^n \prod_{r=1}^{n} \hat{f}(\boldsymbol{e}_{\{r\}}).$$

Now n is odd, so $|S|(n-|S|)$ is even and then

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) \cdot \hat{f}(\boldsymbol{x}) = (-1)^{(n-1)/2}\hat{f}(\mathbf{0}) \prod_{r=1}^{n} \hat{f}(\boldsymbol{e}_{\{r\}}).$$

Now exactly m of the terms $\hat{f}(\mathbf{0}), \hat{f}(\boldsymbol{e}_{\{r\}})$ are equal to -1 and the rest are equal to 1, so

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) \cdot \hat{f}(\boldsymbol{x}) = (-1)^{(n-1)/2}(-1)^m. \qquad \square$$

Proof of Corollary 2.6. By Lemma 2.7, we see that

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) = \hat{f}(\boldsymbol{x}) \oplus 1, \quad \text{for all } \boldsymbol{x} \in \mathbb{Z}_2^n$$

if and only if $(n-1)/2 - m \equiv 1 \pmod 2$. But this congruence can be written as $1 + n - 2m \equiv 0 \pmod 4$ which, by Lemma 2.3, is equivalent to f being balanced. □

3. Uncorrelatedness

We turn now to the question of when functions satisfying the strict avalanche criterion of order $n-2$ are also uncorrelated. There turns out to be a particularly simple formulation when f is also balanced.

Lemma 3.1. *Let $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ and suppose that f is balanced. Then f is uncorrelated if and only if*

$$\sum_{x\in\mathbb{Z}_2^n} \hat{f}(x)\cdot x = (0,\ldots,0).$$

Proof. Since f is balanced, $N=2^n/2=2^{n-1}$. The result then follows from Lemma 1.4. □

If f satisfies the strict avalanche criterion of order $n-2$, then we may use Theorem 1.7 to obtain an expression for $\sum_{x\in\mathbb{Z}_2^n} \hat{f}(x)\cdot x$ as follows.

Lemma 3.2. *Suppose that $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Then, for any j, $1\le j\le n$, the jth component C_j of $\sum_{x\in\mathbb{Z}_2^n} \hat{f}(x)\cdot x$ is equal to*

$$\hat{f}(e_{\{j\}})\Re\left[(1+i\hat{f}(0))\prod_{\substack{r=1\\ r\neq j}}^{n}(1+i\hat{f}(e_{\{r\}}))\right]$$

where $\Re$ denotes the real part.

Proof. Since f satisfies the SAC of order $n-2$, we see that

$$\sum_{x\in\mathbb{Z}_2^n} \hat{f}(x)\cdot x = \sum_{S\subseteq\{1,\ldots,n\}}\left[e_S(-1)^{|S|(|S|-1)/2}(\hat{f}(0))^{(|S|+1)}\prod_{r\in S}\hat{f}(e_{\{r\}})\right].$$

Consider the jth component C_j of this sum. Only those S with $j\in S$ will contribute to this component. For each of these S, let us write T for $S\setminus\{j\}$. Then

$$C_j = \sum_{T\subseteq(\{1,\ldots,n\}\setminus\{j\})}\left[(-1)^{|T|(|T|+1)/2}(\hat{f}(0))^{|T|}\hat{f}(e_{\{j\}})\prod_{r\in T}\hat{f}(e_{\{r\}})\right].$$

Each of the terms in this sum is equal to $\hat{f}(e_{\{j\}})$ multiplied by a product of an even number t of elements of the set $\{\hat{f}(0),\hat{f}(e_{\{1\}}),\ldots,\hat{f}(e_{\{j-1\}}),\hat{f}(e_{\{j+1\}}),\ldots,\hat{f}(e_{\{n\}})\}$ and by $(-1)^{t/2}$. These are exactly the terms which appear in the expansion of the real part of the product above. □

Corollary 3.3. *Suppose that $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Suppose further that exactly m of the input vectors $0, e_{\{r\}}$ are mapped by $\hat{f}$ to -1. Then, for any j, $1\le j\le n$, the jth component C_j of $\sum_{x\in\mathbb{Z}_2^n} \hat{f}(x)\cdot x$ is given by*

$$C_j = \begin{cases} 2^{n/2}\cos(n-2m)\dfrac{\pi}{4}, & \text{if } \hat{f}(\boldsymbol{e}_{\{j\}}) = 1, \\ -2^{n/2}\cos(n+2-2m)\dfrac{\pi}{4}, & \text{if } \hat{f}(\boldsymbol{e}_{\{j\}}) = -1. \end{cases}$$

Proof. By Lemma 3.2, we know that

$$C_j = \hat{f}(\boldsymbol{e}_{\{j\}})\Re\left[(1+i\hat{f}(\boldsymbol{0}))\prod_{\substack{r=1 \\ r\neq j}}^{n}(1+i\hat{f}(\boldsymbol{e}_{\{r\}}))\right]$$

where $\Re$ denotes the real part. Suppose first that $\hat{f}(\boldsymbol{e}_{\{j\}}) = 1$. Then m of the factors in the product are equal to $1-i$, and the remaining $n-m$ are equal to $1+i$. So

$$C_j = \Re[(1-i)^m(1+i)^{n-m}] = 2^{n/2}\cos(n-2m)\frac{\pi}{4}.$$

On the other hand, if $\hat{f}(\boldsymbol{e}_{\{j\}}) = -1$, then $m-1$ of the factors in the product are equal to $1-i$, and the remaining $n-m+1$ are equal to $1+i$. So

$$C_j = -\Re[(1-i)^{m-1}(1+i)^{n-m+1}] = -2^{n/2}\cos(n+2-2m)\frac{\pi}{4}. \qquad \square$$

We are now able to prove a theorem about the nonexistence of balanced, uncorrelated functions satisfying the strict avalanche criterion of order $n-2$.

Theorem 3.4. *Let n be an odd integer. Then there are no balanced, uncorrelated functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$.*

Proof. By Lemma 3.1, a balanced uncorrelated function f satisfies

$$\sum_{\boldsymbol{x}\in\mathbb{Z}_2^n} \hat{f}(\boldsymbol{x})\cdot\boldsymbol{x} = (0,\ldots,0).$$

By Corollary 3.3, this is equivalent to requiring that, for each j, either $\hat{f}(\boldsymbol{e}_{\{j\}}) = 1$ and $\cos(n-2m)\pi/4 = 0$ or $\hat{f}(\boldsymbol{e}_{\{j\}}) = -1$ and $\cos(n+2-2m)\pi/4 = 0$. But since n is odd, both $n-2m$ and $n+2-2m$ are also odd, and so neither $\cos(n-2m)\pi/4$ nor $\cos(n+2-2m)\pi/4$ can be equal to zero. Hence f cannot be both balanced and uncorrelated. $\square$

Corollary 3.5. *Let n be an odd integer, and suppose that $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Then f is uncorrelated if and only if*

$$f(\boldsymbol{x}\oplus(1,\ldots,1)) = f(\boldsymbol{x}), \quad \text{for all } \boldsymbol{x}\in\mathbb{Z}_2^n.$$

Clearly, if f satisfies the above condition, then it is uncorrelated, since each input vector may be matched with its complement. This is the analogous result to Corollary 2.6 for uncorrelatedness. Again, it is perhaps surprising that the converse is also true.

Proof. By Lemma 2.7, we know that for each $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$, either

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) = \hat{f}(\boldsymbol{x}), \qquad \text{for all } \boldsymbol{x} \in \mathbb{Z}_2^n$$

or

$$\hat{f}(\boldsymbol{x} \oplus (1, \ldots, 1)) = \hat{f}(\boldsymbol{x}) \oplus 1, \quad \text{for all } \boldsymbol{x} \in \mathbb{Z}_2^n.$$

Now if f satisfies the first condition, then f is uncorrelated. If f satisfies the second condition, then f is balanced, by Corollary 2.6. Hence, by Theorem 3.4, f is not uncorrelated. So f is uncorrelated if and only if f satisfies the first condition above. □

Corollary 3.6. *Let n be an odd integer. Then exactly half of the functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$ are also uncorrelated.*

Proof. As in the proof of Corollary 3.5, if f satisfies the SAC of order $n-2$, then either f is balanced, or f is uncorrelated, but not both. Hence the number of uncorrelated functions satisfying the SAC of order $n-2$ is equal to the number of functions satisfying the SAC of order $n-2$ minus the number of balanced functions satisfying the SAC of order $n-2$. By Theorem 2.5, this is equal to

$$2^{n+1} - \tfrac{1}{2}2^{n+1} = 2^n = \tfrac{1}{2}2^{n+1}$$

as required. □

Having disposed of the case when n is odd, we turn to the case when n is even.

Theorem 3.7. *Let n be an even integer. Then there are no uncorrelated functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfying the SAC of order $n-2$.*

In order to prove this theorem, we shall calculate $(2^{n-1} - N, \ldots, 2^{n-1} - N)$, where, as usual, N is the size of the inverse image of 1 under f, and show that it can never be equal to $\sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} \hat{f}(\boldsymbol{x})\boldsymbol{x}$.

Proposition 3.8. *Suppose that $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ satisfies the SAC of order $n-2$. Suppose further that exactly m of the input vectors $\mathbf{0}$, $\boldsymbol{e}_{\{r\}}$ are mapped onto 1 by f. Let us write N for the size of the inverse image of 1 under f. Then*

$$2^{n-1} - N = 2^{(n-1)/2} \sin \frac{\pi}{4}(n + 1 - 2m).$$

Proof. By definition, $N = \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} f(\boldsymbol{x})$. Now, by the definition of $\hat{f}$, we know that $f(\boldsymbol{x}) = \frac{1}{2}(1 - \hat{f}(\boldsymbol{x}))$, so

$$N = \tfrac{1}{2} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} (1 - \hat{f}(\boldsymbol{x})) = 2^{n-1} - \tfrac{1}{2} \sum_{\boldsymbol{x} \in \mathbb{Z}_2^n} \hat{f}(\boldsymbol{x}).$$

By Corollary 2.2, therefore,

$$N = 2^{n-1} - \tfrac{1}{2}\, 2^{(n+1)/2} \sin \frac{\pi}{4}(n+1-2m)$$

and so we may deduce the desired result. □

Proof of Theorem 3.7. By Corollary 3.3, the jth component C_j of $\sum_{x \in \mathbb{Z}_2^n} \hat{f}(x) \cdot x$ is given by

$$C_j = \begin{cases} 2^{n/2} \cos(n-2m)\dfrac{\pi}{4}, & \text{if } \hat{f}(e_{\{j\}}) = 1, \\ -2^{n/2} \cos(n+2-2m)\dfrac{\pi}{4}, & \text{if } \hat{f}(e_{\{j\}}) = -1. \end{cases}$$

Since n is even, this means that $C_j = 0$ or $C_j = \pm 2^{n/2}$. By Proposition 3.8, on the other hand,

$$2^{n-1} - N = 2^{(n-1)/2} \sin \frac{\pi}{4}(n+1-2m),$$

and, since n is even, this implies that $2^{n-1} - N = \pm 2^{(n-2)/2}$. These two expressions can never be equal, so f cannot be uncorrelated. □

Conclusions

We have investigated the connections between the three properties of balance, uncorrelatedness and higher order strict avalanche criterion for functions $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$. We have shown that, in the case when n is even, if f satisfies the strict avalanche criterion of order $n-2$, then f is neither balanced nor uncorrelated. We have also shown that, in the case when n is odd, exactly half of the functions satisfying the strict avalanche criterion of order $n-2$ are balanced and the other half are uncorrelated. This means, in particular, that no function is balanced, uncorrelated and satisfies the strict avalanche criterion of order $n-2$. This calls into question the usefulness of this criterion since it is incompatible with simultaneous balance and uncorrelatedness, both of which seem eminently desirable cryptographic properties.

References

[1] R. Forré, The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition, in: Advances in Cryptology, Proceedings CRYPTO88 (Springer, Heidelberg, 1990) 450–468.

[2] S.A. Lloyd, Counting functions satisfying a higher order strict avalanche criterion, in: Abstracts Eurocrypt 89.

[3] A.F. Webster and S.E. Tavares, On the design of S-boxes, in: Advances in Cryptology, Proceedings CRYPTO85 (Springer, Heidelberg, 1986) 523–534.